Posudok vedúceho práce na diplomovú prácu

Daniel Štumpf

Cryptoanalysis of a Post-quantum Cryptography Algorithm

Predložená diplomová práce sa venuje krypto-analýze algoritmu post-kvantovej kryptografie (PQC).

Cieľom študenta bolo naštudovať triedy algoritmov PQC prihlásených do súťaže NIST Post-Quantum Cryptography Standardization Project (PQCSP), vybrať si jednu z kategórii a na ňu sa bližšie zamerať.

V prvej časti práce diplomant popisuje všetky kategórie algoritmov v PQCSP. Pre každú kategóriu uvádza základy teórie na ktorej algoritmy danej triedy stavajú svoju bezpečnosť, stručný popis vybraného algoritmu, jeho bezpečnosť a porovnanie s ostatnými triedami algoritmov. Na koniec prvej kapitoly študent uvádza tabuľky porovnávajúce vybrané vlastnosti implementácii algoritmov v PQCSP. Tie sú podstatné pre ich nasadenie v praxi a ukazujú obmedzenia niektorých tried, ako napríklad príliš náročný výpočet alebo príliš dlhé verejné kľúče. Prvá časť práce poskytuje dobrý prehľad o algoritmoch PQC.

Po štúdiu všetkých tried algoritmov v PQCSP si študent vybral k bližšej analýze algoritmy založené na mriežkových problémoch (Lattice-based Cryptography - LBC). Druhá kapitola začína popisom mriežkových problémov ako SIS, LWE, SVP a CVP. Nasleduje popis prvotného a druhotného útoku (Primal and Dual Attack) a obecná analýza ich zložitosti a aplikovateľnosti voči LBC algoritmom, pričom študent upravil niektoré odhady uvedené v literatúre. Kapitolu zakončujú tabuľky uvádzajúce zložitosti prvotného a druhotného útoku voči vybraných LBC algoritmom v PQCSP uvedené v literatúre a odvodené v práci.

Diplomant zadanie práce splnil. Práca je dobre čitateľná - okrem popisu algoritmov a útokov obsahuje aj základy teórie potrebné k ich pochopeniu. Študentovi sa bohužiaľ nepodarilo prísť s vylepšením žiadneho z popísaných útokov, čo ale nie je možné hodnotiť negatívne.

Prácu navrhujem uznať ako diplomovú a hodnotiť ju známkou *výborně*.

Praha, 17. 6. 2020 Michal Hojsík